Software Rights Archive, LLC v. Google Inc. et al Doc. 129

THE
DEPARTED
JANUARY 26
GOLDEN GLOBE
WINNER
BEST DIRECTOR
MARTIN SCORSESE
R

http://www.salon.com/news/feature/2006/06/21/att_nsa/print.html

salon.com

To print this page, select "Print" from the File menu of your browser

Is the NSA spying on U.S. Internet traffic?

Salon exclusive: Two former AT&T employees say the telecom giant has maintained a secret, highly secure room in St. Louis since 2002. Intelligence experts say it bears the earmarks of a National Security Agency operation.

By Kim Zetter

Jun. 21, 2006 | In a pivotal network operations center in metropolitan St. Louis, AT&T has maintained a secret, highly secured room since 2002 where government work is being conducted, according to two former AT&T workers once employed at the center.

In interviews with Salon, the former AT&T workers said that only government officials or AT&T employees with top-secret security clearance are admitted to the room, located inside AT&T's facility in Bridgeton. The room's tight security includes a biometric "mantrap" or highly sophisticated double door, secured with retinal and fingerprint scanners. The former workers say company supervisors told them that employees working inside the room were "monitoring network traffic" and that the room was being used by "a government agency."

The details provided by the two former workers about the Bridgeton room bear the distinctive earmarks of an operation run by the National Security Agency, according to two intelligence experts with extensive knowledge of the NSA and its operations. In addition to the room's high-tech security, those intelligence experts told Salon, the exhaustive vetting process AT&T workers were put through before being granted top-secret security clearance points to the NSA, an agency known as much for its intense secrecy as its technological sophistication.

"It was very hush-hush," said one of the former AT&T workers. "We were told there was going to be some government personnel working in that room. We were told, 'Do not try to speak to them. Do not hamper their work. Do not impede anything that they're doing.'"

The importance of the Bridgeton facility is its role in managing the "common backbone" for all of AT&T's Internet operations. According to one of the former workers, Bridgeton serves as the technical command center from which the company manages all the routers and circuits carrying the company's domestic and international Internet traffic. Therefore, Bridgeton could be instrumental for conducting surveillance or collecting data.

If the NSA is using the secret room, it would appear to bolster recent allegations that the agency has been conducting broad and possibly illegal domestic surveillance and data collection operations authorized by the Bush administration after the terrorist attacks of Sept. 11, 2001. AT&T's Bridgeton location would give the NSA potential access to an enormous amount of Internet data -- currently, the telecom giant controls approximately one-third of all bandwidth carrying Internet traffic to homes and businesses across the United

Dockets.Justia.com

States.

The nature of the government operation using the Bridgeton room remains unknown, and could be legal. Aside from surveillance or data collection, the room could conceivably house a federal law enforcement operation, a classified research project, or some other unknown government operation.

The former workers, both of whom were approached by and spoke separately to Salon, asked to remain anonymous because they still work in the telecommunications industry. They both left the company in good standing. Neither worked inside the secured room or has access to classified information. One worked in AT&T's broadband division until 2003. The other asked to be identified only as a network technician, and worked at Bridgeton for about three years.

The disclosure of the room in Bridgeton follows assertions made earlier this year by a former AT&T worker in California, Mark Klein, who revealed that the company had installed a secret room in a San Francisco facility and reconfigured its circuits, allegedly to help collect data for use by the government. In detailed documents he provided to the Electronic Frontier Foundation, Klein also alleged there were other secret rooms at AT&T facilities in other U.S. cities.

NSA expert Matthew Aid, who has spent the last decade researching a forthcoming three-volume history of the agency, said of the Bridgeton room: "I'm not a betting man, but if I had to plunk $100 down, I'd say it's safe that it's NSA." Aid told Salon he believes the secret room is likely part of "what is obviously a much larger operation, or series of interrelated operations" combining foreign intelligence gathering with domestic eavesdropping and data collection.

"You're talking about a backbone for computer communications, and that's NSA," Russ Tice, a former high-level NSA intelligence officer, told Salon. Tice, a 20-year veteran of multiple U.S. intelligence agencies, worked for the NSA until spring 2005. "Whatever is happening there with the security you're talking about is a whole lot more closely held than what's going on with the Klein case" in San Francisco, he said. (The San Francisco room is secured only by a special combination lock, according to the Klein documents.)

Tice added that for an operation requiring access to routers and gateways, "the obvious place to do it is right at the source."

In a statement provided to Salon, NSA spokesman Don Weber said: "Given the nature of the work we do, it would be irresponsible to comment on actual or alleged operational issues as it would give those wishing to do harm to the United States insight that could potentially place Americans in danger; therefore, we have no information to provide. However, it is important to note that NSA takes its legal responsibilities seriously and operates within the law."

Since last December, news reports have asserted that the NSA has conducted warrantless spying on the phone and e-mail communications of thousands of people inside the U.S., and has been secretly collecting the phone call records of millions of Americans, using data provided by major telecommunications companies, including AT&T. Such operations would represent a fundamental shift in the NSA's secretive mission, which over the last three decades is widely understood to have focused exclusively on collecting signals intelligence from abroad.

The reported operations have sparked fierce protest by lawmakers and civil liberties advocates, and have raised fundamental questions about the legality of Bush administration policies, including their consequences for the privacy rights of Americans. The Bush administration has acknowledged the use of domestic surveillance operations since Sept. 11, 2001, but maintains they are conducted within the legal authority of the presidency. Several cases challenging the legality of the alleged spying operations are now pending in federal court, including suits against the federal government, and AT&T, among other telecom companies.

In a statement provided to Salon, AT&T spokesman Walt Sharp said: "If and when AT&T is asked by government agencies for help, we do so strictly within the law and under the most stringent conditions. Beyond that, we can't comment on matters of national security."

According to the two former AT&T workers and the Klein documents, the room in the pivotal Bridgeton facility was set up several months before the room in San Francisco. According to the Klein documents, the work order for the San Francisco room came from Bridgeton, suggesting that Bridgeton has a more integral role in operations using the secured rooms.

The company's Bridgeton network operations center, where approximately 100 people work, is located inside a one-story brick building with a small two-story addition connected to it. The building shares a parking lot with a commercial business and is near an interstate highway.

According to the two former workers, the secret room is an internal structure measuring roughly 20 feet by 40 feet, and was previously used by employees of the company's WorldNet division. In spring 2002, they said, the company moved WorldNet employees to a different part of the building and sealed up the room, plastering over the window openings and installing steel double doors with no handles for moving equipment in and out of the room. The company then installed the high-tech mantrap, which has opaque Plexiglas-like doors that prevent anyone outside the room from seeing clearly into the mantrap chamber, or the room beyond it. Both former workers say the mantrap drew attention from employees for being so high-tech.

Telecom companies commonly use mantraps to secure data storage facilities, but they are typically less sophisticated, requiring only a swipe card to pass through. The high-tech mantrap in Bridgeton seems unusual because it is located in an otherwise low-key, small office building. Tice said it indicates "something going on that's very important, because you're talking about an awful lot of money" to pay for such security measures.

The vetting process for AT&T workers granted access to the room also points to the NSA, according to Tice and Aid.

The former network technician said he knows at least three AT&T employees who have been working in the room since 2002. "It took them six months to get the top-security clearance for the guys," the network technician said. "Although they work for AT&T, they're actually doing a job for the government." He said that each of them underwent extensive background checks before starting their jobs in the room. The vetting process included multiple polygraph tests, employment history reviews, and interviews with neighbors and school instructors, going as far back as elementary school.

Aid said that type of vetting is precisely the kind NSA personnel who receive top-secret SCI (Sensitive Compartmented Information) clearance go through. "Everybody who works at NSA has an SCI clearance," said Aid.

It's possible the Bridgeton room is being used for a federal law enforcement operation. According to the Communications Assistance for Law Enforcement Act of 1994, telecom companies are required to assist law enforcement officials who have legal authorization to conduct electronic surveillance, either in pursuit of criminal suspects or for the protection of national security. The companies must design or modify their systems to make such surveillance possible, essentially by making them wiretap-ready.

The FBI is the primary federal agency that tracks and apprehends terrorist suspects within the U.S. Yet, there are several indications that the Bridgeton room does not involve the FBI.

"The FBI, which is probably the least technical agency in the U.S. government, doesn't use mantraps," Aid said. "But virtually every area of the NSA's buildings that contain sensitive operations require you to go through a mantrap with retinal and fingerprint scanners. All of the sensitive offices in NSA buildings have them." The description of the opaque Plexiglas-like doors in Bridgeton, Aid said, indicates that the doors are likely infused with Kevlar for bulletproofing -- another signature measure that he said is used to secure NSA facilities: "You could be inside and you can't kick your way out. You can't shoot your way out. Even if you put plastique explosives, all you could do is blow a very small hole in that opaque glass."

Jameel Jaffer, deputy director of the American Civil Liberties Union's national security program, said it is unlikely that the FBI would set up an ongoing technical operation -- in this case, for several years running -- inside a room of a telecommunications company. The Foreign Intelligence Surveillance Act, passed by Congress in 1978, requires law enforcement officials to obtain warrants from a secret federal court for domestic surveillance operations involving the protection of national security. If the FBI (or another federal agency) wanted data, it would more likely be targeting a specific individual or set of individuals suspected of engaging in criminal or terrorist activities. The agency would obtain a warrant and then call AT&T, or show up in person with the warrant and ask for the wiretap to be engaged. According to Jaffer, the FBI, NSA or any other federal agency could also legally tap into communications data under federal guidelines using technical means that would not require technical assistance of a telecom company.

In an e-mail statement to Salon, FBI spokesperson Paul Bresson said: "The FBI does not confirm whether or not we are involved in an alleged ongoing operational activity. In all cases, FBI operations are conducted in strict accordance with established Department of Justice guidelines, FBI policy, and the law."

Rather than specifically targeted surveillance, it is also possible that the Bridgeton room is being used for a classified government project, such as data mining, with which the Pentagon has experimented in the past. Data mining uses automated methods to search through large volumes of data, looking for patterns that might help identify terrorist suspects, for example. According to Tice, private sector employees who work on classified government projects for the NSA are required to undergo the same kind of top-secret security clearance that AT&T workers in the Bridgeton room underwent.

According to the former network technician, all three AT&T employees he knows who work inside the room have network technician and administration backgrounds -- not research backgrounds -- suggesting that those workers are only conducting maintenance or technical operations inside the room.

Furthermore, Tice said it is much more likely that any classified project using data collected via a corporate facility would take place in separate facilities: "The information that you garner from something like a room siphoning information and filtering it would be sent to some place where you'd have people thinking about what to do with that data," he said.

Dave Farber, a respected computer scientist at Carnegie Mellon University and former chief technologist for the Federal Communications Commission, also said it is likely that data collected in a facility like the Bridgeton center would be used elsewhere, once the facility is set up to divert the data. "If I own the routers, I can put code in there to have them monitor for certain data. That's not a particularly difficult job," said Farber, who is considered one of the pioneers of Internet architecture. Farber said that "packets" of data can essentially be copied and then sent to some other location for use. "Most of the problems would have to do with keeping your staff from knowing too much about it."

According to the former network technician, workers at Bridgeton, at the direction of government officials, could conceivably collect data using any AT&T router around the country, which he says number between 1,500 and 2,000. To do so, the company would need to install a wiretap-like device at select locations for "sniffing" the desired data. That could explain the purpose of the San Francisco room divulged by Klein, as well as the secret rooms he alleged existed at AT&T facilities in other U.S. cities.

"The network sniffer with the right software can capture anything," the former network technician said. "You can get people's e-mail, VoIP phone calls, [calls made over the Internet] -- even passwords and credit card transactions -- as long as you have the right software to decrypt that."

In theory, surveillance involving Internet communications can be executed legally under federal law. "But with most of these things," Farber said, "the problem is that it just takes one small step to make it illegal."

-- By Kim Zetter

Salon | About Salon | Contact & Help | Corrections | Advertise in Salon | Salon Personals
Salon Mobile | Salon Newsletter | RSS Feeds

Salon Premium: Premium log in | What is Salon Premium?

From the directory: Ban | Martin Luther King Jr. | Holland | Spies | South Korea | Mexico
Thailand | Palestine | Coup | South Africa | Bali | Tibet | England | Greece

A & E | Books | Comics | Community: Table Talk & The WELL | Life | News & Politics
Opinion | Sports | Tech & Business | Letters

Investor Relations | Privacy Policy | Terms of Service
Copyright ©2007 Salon Media Group, Inc. Reproduction of material from any Salon pages without written permission is strictly prohibited. SALON® is registered in the U.S. Patent and Trademark Office as a trademark of Salon Media Group Inc.